The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE (S) ISSUED:

02/08/2011

SUBJECT:

Multiple Vulnerabilities in Internet Explorer Could Allow Remote Code Execution (MS11-003)

OVERVIEW:

Multiple vulnerabilities have been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

D**ESCRIPTION:**

Four vulnerabilities have been discovered in Microsoft Internet Explorer. Details of these vulnerabilities are as follows:

CSS Memory Corruption Vulnerability

A remote code execution vulnerability exists in the way Internet Explorer accesses memory when importing a recursive Cascading Styling Sheet (CSS). This vulnerability may be exploited if a user visits a web page that is specifically crafted to take advantage of the vulnerability. Successful exploitation could result in an attacker taking complete control of the system.

Uninitialized Vulnerabilities

Two remote code execution vulnerabilities exist in the way that Internet Explorer accesses an object that has not been correctly initialized or has been deleted. Exploitation may occur if a user visits a web page that is specifically crafted to take advantage of these vulnerabilities.

Insecure Library Loading Vulnerability

A remote code execution vulnerability exists in the way Internet Explorer loads DLL files. Three different scenarios exists for an attack on this vulnerability to be successful:

- In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a legitimate HTML file and specially crafted DLL attachments to a user, and persuade the user to place the files on the desktop and to open the HTML file. Then, while opening the HTML file, Internet Explorer could attempt to load the DLL file and execute any code it contained.
- In a Web-based attack scenario, an attacker could persuade a user to download and save a legitimate HTML file and specially crafted DLL on to the desktop and persuade the user to open the legitimate HTML file. While opening the HTML file, Internet Explorer could

attempt to load the DLL file and execute any code it contained. This vulnerability could not be exploited by simply browsing to a Web page; user interaction is required.

- In a network attack scenario, an attacker could place a legitimate HTML file and a specially crafted DLL on a network share, such as a UNC or WebDAV location. The attacker would then have to persuade the user to change the PATH environment variable to include this network share, UNC, or WebDAV location and then persuade the user to open the HTML file. Then, while opening the HTML file, Internet Explorer could attempt to load the DLL file found on the search path and execute any code it contained.

Successful exploitation of any of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Please note that this Microsoft bulletin also patches the zero-day vulnerability identified in MS-ISAC Advisory 2010-109.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:

Microsoft:

http://www.microsoft.com/technet/security/bulletin/ms11-003.mspx

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3971

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0035

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0036

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0038

MS-ISAC:

http://www.msisac.org/advisories/2010/2010-109.cfm